

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2002年11月14日
Date of Application:

出願番号 特願2002-330569
Application Number:

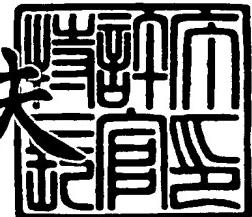
[ST. 10/C] : [JP2002-330569]

出願人 ソニー株式会社
Applicant(s):

2003年 8月25日

特許庁長官
Commissioner,
Japan Patent Office

今井 康夫



【書類名】 特許願

【整理番号】 0290499003

【提出日】 平成14年11月14日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/31

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 菅 真紀子

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100094053

【弁理士】

【氏名又は名称】 佐藤 隆久

【手数料の表示】

【予納台帳番号】 014890

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707389

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 回路構成方法、その方法およびそのプログラム

【特許請求の範囲】

【請求項 1】

有限体上の演算を行う演算回路を構成する回路構成方法であって、

第1の有限体から第2の有限体への第1の拡大についての第1の多項式を基に
第1の原始根 α_1 を得る第1の工程と、

前記第2の有限体から前記第3の有限体への第2の拡大についての第2の多項式であって、前記第1の工程で得られた前記第1の原始根 α_1 と前記第1の多項式の0次の項の係数とを用いて、0次の項の係数が規定された前記第2の多項式を基に第2の原始根 α_2 を得る第2の工程と、

前記第2の工程で得られた前記第2の原始根 α_2 を用いて表現された基底を用いて、前記第3の有限体上の演算を規定する第3の工程と、

前記第3の工程で規定された演算を基に、当該演算を行う演算回路を構成する第4の工程と

を有する回路構成方法。

【請求項 2】

前記第1の有限体が、有限体 F_q から拡大次数 n の拡大であり、

前記第2の有限体が、前記第1の有限体から拡大次数 l_1 の第1の拡大であり

前記第3の有限体が、前記第2の有限体から拡大次数 l_2 の第2の拡大であり

前記第3の工程において、下記（1-1）で示す位数の下記（1-2）で示す前記第3の有限体上の演算を規定する場合に、

前記第1の工程において、前記第1の原始根 α_1 を下記（1-3）を基に得て

前記第2の工程において、前記第2の原始根 α_2 を下記（1-4）を基に得る請求項1に記載の回路構成方法。

【数1】

$$q^{n-l_1-l_2} (q = p^m, p; \text{素数}, n, l_1, l_2, m; \text{自然数}) \cdots (1-1)$$

【数2】

$$L := F_{q^{n-l_1-l_2}} \cdots (1-2)$$

【数3】

$$\alpha_1: \alpha_1^{l_1} - \alpha_1 + c = 0, \quad X^{l_1} - X + c \in F[X], \text{既約} \cdots (1-3)$$

【数4】

$$\begin{aligned} \alpha_2: \alpha_2^{l_2} - \alpha_2 + a &= 0, \quad a = c^{-1} \cdot \alpha_1^i \cdot \exists i \in Z, \\ &\text{s.t. } X^{l_2} - X + a \in K[X], \text{既約} \end{aligned} \cdots (1-4)$$

【請求項3】

前記拡大次数 l_1 と l_2 とが共に q である場合に、

前記第1の工程において、前記第1の原始根 α_1 を下記 (1-5), (1-5a) を基に得て、

前記第2の工程において、前記第2の原始根 α_2 を下記 (1-6) を基に得る
請求項2に記載の回路構成方法。

【数5】

$$\alpha_1: \alpha_1^q - \alpha_1 + c = 0, \quad \exists c \in F \text{ s.t. } Tr_{F_q}(c) \neq 0 \cdots (1-5)$$

【数6】

$$Tr_{F_q}(c) := c + c^q + c^{q^2} + c^{q^3} + \cdots + c^{q^{n-1}} \cdots (1-5a)$$

【数7】

$$\begin{aligned} \alpha_2: \alpha_2^q - \alpha_2 + a &= 0, \quad \exists a = c^{-1} \cdot \alpha_1^i \in K, \\ &i \in Z \text{ s.t. } Tr_{F_q}(\alpha_1^i) \neq 0, \end{aligned} \cdots (1-6)$$

【請求項 4】

前記第3の工程において、前記第2の有限体上の演算を用いて前記第3の有限体上の演算を規定し、

前記第4の工程において、前記第3の工程で用いた前記第2の有限体上の演算を行う第1の演算回路を構成し、当該第1の演算回路を用いて前記第3の有限体上の演算を行う第2の演算回路を構成する

請求項1に記載の回路構成方法。

【請求項 5】

前記第3の工程において、前記第2の多項式の0次の項の係数を乗じる前記第2の有限体上の演算を用いて、前記第3の有限体上の演算を規定する

請求項4に記載の回路構成方法。

【請求項 6】

有限体上の演算を行う演算回路を構成する回路構成装置であって、

第1の有限体から第2の有限体への第1の拡大についての第1の多項式を基に第1の原始根 α_1 を得る第1の手段と、

前記第2の有限体から前記第3の有限体への第2の拡大についての第2の多項式であって、前記第1の手段で得られた前記第1の原始根 α_1 と前記第1の多項式の0次の項の係数とを用いて、0次の項の係数が規定された前記第2の多項式を基に第2の原始根 α_2 を得る第2の手段と、

前記第2の手段で得られた前記第2の原始根 α_2 を用いて表現された基底を用いて、前記第3の有限体上の演算を規定する第3の手段と、

前記第3の手段で規定された演算を基に、当該演算を行う演算回路を構成する第4の手段と

を有する回路構成装置。

【請求項 7】

有限体上の演算を行う演算回路を構成する回路構成装置によって実行されるプログラムであって、

第1の有限体から第2の有限体への第1の拡大についての第1の多項式を基に第1の原始根 α_1 を得る第1の手順と、

前記第2の有限体から前記第3の有限体への第2の拡大についての第2の多項式であって、前記第1の手順で得られた前記第1の原始根 α_1 と前記第1の多項式の0次の項の係数とを用いて、0次の項の係数が規定された前記第2の多項式を基に第2の原始根 α_2 を得る第2の手順と、

前記第2の手順で得られた前記第2の原始根 α_2 を用いて表現された基底を用いて、前記第3の有限体上の演算を規定する第3の手順と、

前記第3の手順で規定された演算を基に、当該演算を行う演算回路を構成する第4の手順と

を有するプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、有限体上の演算を行う演算回路の回路構成方法、その方法およびそのプログラムに関する。

【0002】

【従来の技術】

例えば、ハミング符号などの誤り訂正符号や復号では、例えば、有限体上の演算が行われている。

このような有限体は、他の有限体からの拡大によって規定される場合がある。

例えば、第1の有限体からの第1の拡大によって第2の有限体が規定され、第2の有限体からの第2の拡大によって第3の有限体が規定される場合に、上記第3の有限体上の演算は、上記第2の有限体上の演算を用いて規定される。

また、上記第2の有限体上の演算は、上記第1の拡大についての第1の多項式によって得られた原始根を基に決定された基底を用いて表現される。また、第2の有限体上の演算は、上記第2の拡大についての第2の多項式によって得られた原始根を基に決定された基底を用いて表現される。

従来の回路構成方法では、上記第2の多項式の0次の項の係数を、上記第1の多項式の0次の項の係数とは無関係に定めている。

【0003】

【発明が解決しようとする課題】

しかしながら、上述した従来の回路構成方法では、第3の有限体上の演算を行う演算回路の回路構成要素が多くなり、当該演算回路が大規模化してしまうという問題がある。

【0004】

本発明はかかる事情に鑑みてなされたものであり、有限体上の演算を行う演算回路を従来に比べて少ない回路構成要素で小規模に構成できる回路構成方法、その装置、そのプログラムおよび演算回路を提供することを目的とする。

【0005】**【課題を解決するための手段】**

上記の目的を達成するため、第1の発明の回路構成方法は、有限体上の演算を行う演算回路を構成する回路構成方法であって、第1の有限体から第2の有限体への第1の拡大についての第1の多項式を基に第1の原始根 α_1 を得る第1の工程と、前記第2の有限体から前記第3の有限体への第2の拡大についての第2の多項式であって、前記第1の工程で得られた前記第1の原始根 α_1 と前記第1の多項式の0次の項の係数とを用いて、0次の項の係数が規定された前記第2の多項式を基に第2の原始根 α_2 を得る第2の工程と、前記第2の工程で得られた前記第2の原始根 α_2 を用いて表現された基底を用いて、前記第3の有限体上の演算を規定する第3の工程と、前記第3の工程で規定された演算を基に、当該演算を行う演算回路を構成する第4の工程とを有する。

【0006】

第1の発明の回路構成方法の作用は以下のようになる。

先ず、第1の工程において、第1の有限体から第2の有限体への第1の拡大についての第1の多項式を基に第1の原始根 α_1 を得る。

次に、第2の工程において、前記第2の有限体から前記第3の有限体への第2の拡大についての第2の多項式であって、前記第1の工程で得られた前記第1の原始根 α_1 と前記第1の多項式の0次の項の係数とを用いて、0次の項の係数が規定された前記第2の多項式を基に第2の原始根 α_2 を得る。

次に、第3の工程において、前記第2の工程で得られた前記第2の原始根 α_2

を用いて表現された基底を用いて、前記第3の有限体上の演算を規定する。

次に、第4の工程において、前記第3の工程で規定された演算を基に、当該演算を行う演算回路を構成する。

【0007】

第2の発明の回路構成装置は、有限体上の演算を行う演算回路を構成する回路構成装置であって、第1の有限体から第2の有限体への第1の拡大についての第1の多項式を基に第1の原始根 α_1 を得る第1の手段と、前記第2の有限体から前記第3の有限体への第2の拡大についての第2の多項式であって、前記第1の手段で得られた前記第1の原始根 α_1 と前記第1の多項式の0次の項の係数とを用いて、0次の項の係数が規定された前記第2の多項式を基に第2の原始根 α_2 を得る第2の手段と、前記第2の手段で得られた前記第2の原始根 α_2 を用いて表現された基底を用いて、前記第3の有限体上の演算を規定する第3の手段と、前記第3の手段で規定された演算を基に、当該演算を行う演算回路を構成する第4の手段とを有する。

【0008】

第2の発明の回路構成装置の作用は以下のようになる。

先ず、第1の手段において、第1の有限体から第2の有限体への第1の拡大についての第1の多項式を基に第1の原始根 α_1 を得る。

次に、第2の手段において、前記第2の有限体から前記第3の有限体への第2の拡大についての第2の多項式であって、前記第1の手段で得られた前記第1の原始根 α_1 と前記第1の多項式の0次の項の係数とを用いて、0次の項の係数が規定された前記第2の多項式を基に第2の原始根 α_2 を得る。

次に、第3の手段において、前記第2の手段で得られた前記第2の原始根 α_2 を用いて表現された基底を用いて、前記第3の有限体上の演算を規定する。

次に、第4の手段において、前記第3の手段で規定された演算を基に、当該演算を行う演算回路を構成する。

【0009】

第3の発明のプログラムは、有限体上の演算を行う演算回路を構成する回路構成装置によって実行されるプログラムであって、第1の有限体から第2の有限体

への第1の拡大についての第1の多項式を基に第1の原始根 α_1 を得る第1の手順と、前記第2の有限体から前記第3の有限体への第2の拡大についての第2の多項式であって、前記第1の手順で得られた前記第1の原始根 α_1 と前記第1の多項式の0次の項の係数とを用いて、0次の項の係数が規定された前記第2の多項式を基に第2の原始根 α_2 を得る第2の手順と、前記第2の手順で得られた前記第2の原始根 α_2 を用いて表現された基底を用いて、前記第3の有限体上の演算を規定する第3の手順と、前記第3の手順で規定された演算を基に、当該演算を行う演算回路を構成する第4の手順とを有する。

【0010】

【発明の実施の形態】

〔本発明の関連技術〕

当該関連技術では、有限体 F が有限体 F_q の n 次拡大であり、有限体 K が有限体 F からの拡大次数 q の拡大であり、有限体 L が有限体 K からの拡大次数 q の拡大である場合に、有限体 K 上の a 倍演算を含む有限体 L 上の演算を行う演算回路を構成する回路構成方法を説明する。

ここで、位数が下記（2-1）で示され、有限体 L が下記（2-2）のように表現される。本実施形態では、下記（2-1），（2-2）において、 $l_1 = 1$
 $l_2 = q$ の場合を例示する。

この場合に、上記拡大の関係は、下記（2-3）で示される。

【0011】

【数8】

$$q^{n \cdot l_1 \cdot l_2} (q = p^m, p; \text{素数}, n, l_1, l_2, m; \text{自然数}) \quad \cdots (2-1)$$

【0012】

【数9】

$$L := F_{q^{n \cdot l_1 \cdot l_2}} \quad \cdots (2-2)$$

【0013】

【数10】

$$(F_q \subset) \quad F \subset K \subset L \quad \cdots (2-3)$$

n次 ⁽¹⁾_q次拡大 ⁽²⁾_q次拡大

【0014】

従来の回路構成方法では、図1に示すように、有限体K上の12次元ベクトルD_INを入力し、有限体K上の12次元ベクトルD_OUTを出力し、有限体K上のa倍演算回路301を有し、有限体L上の演算を行う演算回路300を構成する。

有限体K上のa倍演算回路301は、有限体F上の11次元ベクトルVAを入力し、有限体F上の11次元ベクトルVDを出力する。

有限体Fから有限体Kへの第1の拡大K/Fの原始根 α_1 を下記(2-4)に示す第1の多項式を基に得る。

そして、原始根 α_1 を基に、有限体K上の演算の基底を選択する。

【0015】

【数11】

$$\alpha_1: \alpha_1^q - \alpha_1 + c = 0, \quad \exists c \in F \text{ s.t. } Tr_{F_q}^F(c) \neq 0, \quad \cdots (2-4)$$

【0016】

また、有限体Kから有限体Lへの第2の拡大L/Kの原始根 α_2 を下記(2-5)に示す第2の多項式を基に得る。

そして、原始根 α_2 を基に、有限体L上の演算の基底を選択する。

ここで、上記a倍演算回路301のaは、下記(2-5)内の0次の項の係数aである。

【0017】

【数12】

$$\alpha_2 : \alpha_2^q - \alpha_2 + a = 0, \quad \exists a = d \cdot \alpha_1^i \in K,$$

$$i \in Z \text{ s.t. } Tr_{F_q}^K(\alpha_1^i) \neq 0, \quad \cdots (2-5)$$

【0018】

そして、上記原始根 α_1 を基に定められた基底を用いた下記 (2-6) に示す有限体K上の任意の元Aを、下記 (2-7) のように有限体F上の一₁ (= q) 次元ベクトルVAで示す。

【0019】

【数13】

$$A : A_0 + A_1\alpha_1 + A_2\alpha_1^2 + \cdots + A_{q-1}\alpha_1^{q-1} \quad \cdots (2-6)$$

【0020】

【数14】

$$VA := (A_0, A_1, A_2, \dots, A_{q-1}) \quad \cdots (2-7)$$

【0021】

また、上記原始根 α_1 を基に定められた基底を用いた下記 (2-8) で示すDを、下記 (2-9) のように有限体F上の一₁ (= q) 次元ベクトルVDで示す。

【0022】

【数15】

$$D := a \cdot A = D_0 + D_1\alpha_1 + D_2\alpha_1^2 + \cdots + D_{q-1}\alpha_1^{q-1} \quad \cdots (2-8)$$

【0023】

【数16】

$$VD := (D_0, D_1, D_2, \dots, D_{q-1}) \quad \cdots (2-9)$$

【0024】

この場合に、 $D := a \cdot A$ は、上記 (2-5) で定義される a 、並びに上記 (2-6) で定義される A を用いると、下記 (2-10) のように示され、ベクトル VD は下記 (2-11) のように示される。ここで、下記 (2-12) の左辺の α_1^q の q 乗値を右辺の値 ($\alpha_1^q - 1$) に置き換えて表現される。

【0025】

【数17】

$$\begin{aligned}
 & -cd \cdot A_{q-i} \cdot \alpha_1^0 + \sum_{k=1}^{i-1} \left\{ (d \cdot A_{k+q-i-1} - cd \cdot A_{k+q-i}) \cdot \alpha_1^k \right\} \\
 & + d(A_0 + A_{q-1}) \cdot \alpha_1^i + d \sum_{k=i+1}^{q-1} \left\{ A_{k-i} \cdot \alpha_1^k \right\} \quad \cdots (2-10)
 \end{aligned}$$

【0026】

【数18】

$$\begin{aligned}
 & \left\{ -cdA_{q-i}, dA_{1+q-i-1} - cdA_{1+q-i}, dA_{2+q-i-1} - cdA_{2+q-i}, \dots \right. \\
 & \left. \dots, dA_{i-1+q-i-1} - cdA_{i-1+q-i}, d(A_0 + A_{q-1}), dA_{i+1-i}, dA_{i+2-i}, \dots, dA_{q-1-i} \right\} \quad \cdots (2-11)
 \end{aligned}$$

【0027】

【数19】

$$\alpha_1^q = \alpha_1 - c \quad \cdots (2-12)$$

【0028】

上記回路構成方法では、上記 (2-10), (2-11) を基に、図2に示すように、図1に示す有限体 K 上の a 倍演算回路 301 を構成する。

図2に示す a 倍演算回路 301 には、上記 (2-7) で示す q 次元ベクトル V A が入力される。

図2に示す $A[0] \sim A[q-1]$ が、上記 (2-7) に示す $A_0 \sim A_{q-1}$ にそれぞれ対応している。

a 倍演算回路 301 は、上記 (2-4) より得られる下記 (2-12) を基に

α_1 の q 次の項を 1 次および 0 次の項で置き換えて上記 (2-10) に示す演算を行うように構成される。

これにより、a 倍演算回路 301 は、 α_1 の q 次未満の項の係数についての演算を行うように構成される。

【0029】

図 2 に示すように、上記回路構成方法は、データ $A[0] \sim A[q-1]$ のそれぞれが、係数 d を乗算する $q-1$ 個の乗算回路 $31_1 \sim 31_{q-1}$ 、係数 c_d を乗算する $i-1$ 個の乗算回路 $32_1 \sim 32_{i-1}$ 、加算回路 33 のうち、対応する回路に入力されるように a 倍演算回路 301 を構成する。

また、上記回路構成方法は、乗算回路 $32_0 \sim 32_{i-1}$ の出力が、インバータ $35_0 \sim 35_{i-1}$ にそれぞれ入力されるように a 倍演算回路 301 を構成する。

また、上記回路構成方法は、乗算回路 $31_1 \sim 31_{i-1}$ の出力が、それぞれ加算回路 $34_1 \sim 34_{i-1}$ に入力されるように a 倍演算回路 301 を構成する。

また、上記回路構成方法は、インバータ $35_1 \sim 35_{i-1}$ の出力が、それぞれ加算回路 $34_1 \sim 34_{i-1}$ に入力されるように a 倍演算回路 301 を構成する。

また、上記回路構成方法は、乗算回路 33 の出力が、係数 d を乗算する乗算回路 32 に入力されるように a 倍演算回路 301 を構成する。

そして、インバータ 35_0 、加算回路 $34_1 \sim 34_{i-1}$ 、乗算回路 32、並びに乗算回路 $31_i \sim 31_{q-1}$ の出力が、それぞれデータ $D[0] \sim [q-1]$ となる。

図 2 に示す $D[0] \sim D[q-1]$ が、上記 (2-9), (2-11) に示す $D_0 \sim D_{q-1}$ にそれぞれ対応している。

【0030】

[発明の実施の形態]

本実施形態では、上述した関連技術と同様に、有限体 F (本発明の第 1 の有限体) が有限体 F_q の n 次拡大であり、有限体 K (本発明の第 2 の有限体) が有限

体Fからの拡大次数qの拡大であり、有限体L（本発明の第3の有限体）が有限体Kからの拡大次数qの拡大である場合に、有限体K上のa倍演算を含む有限体L上の演算を行う演算回路を構成する回路構成方法を説明する。

ここで、位数が下記（3-1）で示され、有限体Lが下記（3-2）のように表現される。本実施形態では、下記（3-1），（3-2）において、 $l_1 = l_2 = q$ の場合を例示する。例えば、qは2、nは4である。

この場合に、上記拡大の関係は、下記（3-3）で示される。

【0031】

【数20】

$$q^{n \cdot l_1 \cdot l_2} (q = p^m, p: \text{素数}, n, l_1, l_2, m: \text{自然数}) \quad \cdots (3-1)$$

【0032】

【数21】

$$L := F_{q^{n \cdot l_1 \cdot l_2}} \quad \cdots (3-2)$$

【0033】

【数22】

$$(F_q \subset) \quad F \overset{(1)}{\subset} K \overset{(2)}{\subset} L \quad \cdots (3-3)$$

【0034】

本実施形態の回路構成方法では、図3に示すように、有限体K上の $l_2 (= q)$ 次元ベクトルD_INを入力し、有限体K上の l_2 次元ベクトルD_OUTを出力し、有限体K上のa倍演算回路101を有し、有限体L上の演算を行う演算回路100を構成する。

有限体K上のa倍演算回路101は、有限体F上の $l_1 (= q)$ 次元ベクトルVAを入力し、有限体F上の l_1 次元ベクトルVDを出力する。

有限体Fから有限体Kへの第1の拡大 K/F （本発明の第1の拡大）の第1の原始根 α_1 （本発明の第1の原始根）を下記（3-4）に示す第1の多項式を得る。

そして、原始根 α_1 を基に、有限体 K 上の演算の基底を選択する。

【0035】

【数23】

$$\alpha_1: \alpha_1^q - \alpha_1 + c = 0, \quad \exists c \in F \text{ s.t. } Tr_{F_q}^F(c) \neq 0, \quad \cdots (3-4)$$

【0036】

上記 (3-4) において、トレース Tr は、下記 (3-4a) のように定義される。

【0037】

【数24】

$$Tr_{F_q}^F(c) := c + c^q + c^{q^2} + c^{q^3} + \cdots + c^{q^{n-1}} \quad \cdots (3-4a)$$

【0038】

また、有限体 K から有限体 L への第 2 の拡大 L/K (本発明の第 2 の拡大) の第 2 の原始根 α_2 (本発明の第 2 の原始根) を下記 (3-5) に示す第 2 の多項式 (本発明の第 2 の多項式) を基に得る。

ここで、下記 (3-5) に示す第 2 の多項式は、上記 (3-4) に示す第 1 の多項式の第 1 の原始根 α_1 と当該第 1 の多項式の 0 次の項の係数 c とを用いて、0 次の項の係数 a が規定されている。

【0039】

【数25】

$$\alpha_2: \alpha_2^q - \alpha_2 + a = 0, \quad \exists a = c^{-1} \cdot \alpha_1' \in K, \\ i \in Z \text{ s.t. } Tr_{F_q}^K(\alpha_1') \neq 0, \quad \cdots (3-5)$$

【0040】

そして、上記第 1 の原始根 α_1 を基に定められた基底を用いた下記 (3-6) に示す有限体 K 上の任意の元 A を、下記 (3-7) のように有限体 F 上の 1 次元ベクトル VA で示す。

【0041】

【数26】

$$A: A_0 + A_1\alpha_1 + A_2\alpha_1^2 + \cdots + A_{q-1}\alpha_1^{q-1} \quad \cdots (3-6)$$

【0042】

【数27】

$$VA := (A_0, A_1, A_2, \dots, A_{q-1}) \quad \cdots (3-7)$$

【0043】

また、上記第1の原始根 α_1 を基に定められた基底を用いた下記 (3-8) で示すDを、下記 (3-9) のように有限体F上の11次元ベクトルVDで示す。

【0044】

【数28】

$$D := a \cdot A = D_0 + D_1\alpha_1 + D_2\alpha_1^2 + \cdots + D_{q-1}\alpha_1^{q-1} \quad \cdots (3-8)$$

【0045】

【数29】

$$VD := (D_0, D_1, D_2, \dots, D_{q-1}) \quad \cdots (3-9)$$

【0046】

この場合に、 $D := a \cdot A$ は、上記 (3-5) で定義される a 、並びに上記 (3-6) で定義される A を用いると、下記 (3-10) のように示され、ベクトル $D \in V$ は下記 (3-11) で示される。ここで、上記 (3-4) から得られる下記 (3-12) の左辺の α_1 の q 乗値を右辺の値 ($\alpha_1 - 1$) に置き換えて表現される。

【0047】

【数30】

$$D := a \cdot A$$

$$\begin{aligned}
 &= -A_{l_1-i} \cdot \alpha_1^0 + \sum_{k=1}^{j-1} \left\{ (c^{-1} \cdot A_{k+l_1-i-1} - A_{k+l_1-i}) \cdot \alpha_1^k \right\} \\
 &+ c^{-1}(A_0 + A_{l_1-1}) \cdot \alpha_1^j + c^{-1} \sum_{k=j+1}^{l_1-1} \left\{ A_{k-i} \cdot \alpha_1^k \right\} \quad \cdots (3-10)
 \end{aligned}$$

【0048】

【数31】

$$\begin{aligned}
 &(-A_{l_1-i}, c^{-1}A_{1+l_1-i-1} - A_{1+l_1-i}, c^{-1}A_{2+l_1-i-1} - A_{2+l_1-i}, \dots \\
 &\dots, c^{-1}A_{i-1+l_1-i-1} - A_{i-1+l_1-i}, c^{-1}(A_0 + A_{l_1-1}), \\
 &c^{-1}A_{i+l_1-i}, c^{-1}A_{i+2-i}, \dots, c^{-1}A_{l_1-1-i})
 \end{aligned} \quad \cdots (3-11)$$

【0049】

【数32】

$$\alpha_1^q = \alpha_1 - c \quad \cdots (3-12)$$

【0050】

上記回路構成方法では、上記(3-10), (3-11)を基に、図1に示すように、有限体K上のa倍演算回路101を構成する。

ここで、a倍演算回路101のaは、上記(3-5)内のaである。

【0051】

図4は、本実施形態の回路構成方法を実行するコンピュータ29(本発明の回路構成装置)の構成図である。

図4に示すように、コンピュータ29は、例えば、操作部31、ディスプレイ32、メモリ33およびCPU34を有し、これらがバス30を介して接続されている。

操作部31は、キーボードやマウスなどの操作手段であり、ユーザの操作に応じた操作信号をCPU34に出力する。

ディスプレイ32は、CPU34による回路構成の処理に応じた画面を表示する。

メモリ33は、CPU34の処理に用いられるプログラム41（本発明のプログラム）およびデータ42を記憶する。

【0052】

CPU34は、プログラム41を実行し、データ42を用いて、以下に示すように上記有限体L上の演算回路における上記有限体K上のa倍演算回路を構成（設計）する。

CPU34が、本発明の回路構成装置の第1～第4の手段に対応している。

【0053】

図5は、CPU34が演算回路2内の各乗算回路を構成する場合の動作例を説明するためのフローチャートである。

ステップST1：

CPU34が、有限体Fから有限体Kへの第1の拡大についての上記（3-4）に示す第1の多項式を基に第1の原始根 α_1 を得る。

【0054】

ステップST2：

CPU34が、ステップST1で得られた第1の原始根 α_1 および第1の多項式の0次の項の係数とを用いてその0次の項の係数aが規定された上記（3-5）に示す第2の多項式を基に上記第2の原始根 α_2 を得る。

【0055】

ステップST3：

CPU34が、ステップST2で得られた上記原始根 α_2 を用いて表現された基底を用いて、有限体L上の演算を規定する。

そして、上記有限体L上の演算内に、上有限体K上のa倍演算がある場合に、上記（3-10），（3-11）を基に、a倍演算を規定する。このとき、上記（3-12）を基に、上記（3-10）における α_1 のq次の項を1次および0次の項の係数cで置き換えて、当該a倍演算を規定する。これにより、上記a倍演算は、 α_1 のq次未満の項の係数についての演算によって規定される。

【0056】

ステップST4；

CPU34が、ステップST3で規定された演算を基に、上記有限体K上のa倍演算回路を含む、有限体L上の上記演算を行う演算回路を構成する。

【0057】

本実施形態では、例えば、図3に示す有限体K上のa倍演算回路101が、図6に示すように構成される。

すなわち、CPU34が、上記(3-7)で示すq次元ベクトルVAを入力するようにa倍演算回路101を構成する。

図6に示すA[0]～A[q-1]が、上記(3-7)に示すA₀～A_{q-1}にそれぞれ対応している。

また、CPU34が、図6に示すように、データA[0]～A[q-1]のそれぞれが、インバータ13_0～13_i-1、c⁻¹倍演算を行うc⁻¹倍演算回路11_1～11_i-1、c⁻¹倍演算回路11_i+1～11_q-1および、加算回路12のうち対応する回路に入力されるようにa倍演算回路101を構成する。

【0058】

また、CPU34が、c⁻¹倍演算回路11_1～11_i-1の出力が加算回路14_1～14_i-1に入力されるようにa倍演算回路101を構成する。

また、CPU34が、インバータ13_1～13_i-1の出力が加算回路14_1～14_i-1に入力されるようにa倍演算回路101を構成する。

【0059】

また、CPU334が、加算回路12の出力がc⁻¹倍演算回路11_iに入力されるようにa倍演算回路101を構成する。

そして、CPU34が、インバータ13_0、加算回路14_1～14_i-1、c⁻¹倍演算回路11_i～11_q-1の出力が、それぞれデータD[0]～[q-1]となるように、a倍演算回路101を構成する。

図6に示すD[0]～D[q-1]が、上記(3-9)，(3-11)に示すD₀～D_{q-1}にそれぞれ対応している。

【0060】

以上説明したように、本実施形態の回路構成方法によれば、上記（3-5）に示すように、第2の多項式の0次の項の係数aを、上記（3-4）に示す第1の多項式の第1の原始根 α_1 と当該第1の多項式の0次の項の係数cとを用いて規定することで、図2に示すa倍演算回路301に比べて、回路数が削減され、小規模化された図6に示すa倍演算回路101を構成できる。図2に示す従来のa倍演算回路301では、X倍演算回路として上記（2-4）に示す係数cと上記（2-5）に示す係数dとに係わる乗算を行う回路が必要だったが、a倍演算回路101では、X倍演算回路は係数cに係わる回路のみとなる。

【0061】

本発明は上述した実施形態には、限定されない。

例えば、上記（3-4），（3-5）において、 $q = 2$ ， $n = 4$ とすると、第1の有限体Fは下記（4-1）で示され、上記（3-4），（3-5）はそれぞれ下記（4-2），（4-3）で示される。

【0062】

【数33】

$$F = F_2(\gamma), \gamma^4 + \gamma + 1 = 0 \quad \cdots(4-1)$$

【0063】

【数34】

$$\alpha_1: \alpha_1^2 + \alpha_1 + c = 0, \quad c = \gamma^3 \quad \cdots(4-2)$$

【0064】

【数35】

$$\alpha_2: \alpha_2^2 + \alpha_2 + a = 0, \quad a = \gamma^{-3} \cdot \alpha_1 \quad \cdots(4-3)$$

【0065】

また、上述した実施形態では、K上のa倍演算回路を含むL上の演算回路を構成する場合を例示したが、本発明は、その他、K上の乗算回路または逆元生成回

路を含むL上の演算回路を構成してもよい。

【0066】

【発明の効果】

本発明によれば、有限体上の演算を行う演算回路を従来に比べて少ない回路構成要素で小規模に構成できる回路構成方法、その装置、そのプログラムおよび演算回路を提供することができる。

【図面の簡単な説明】

【図1】

図1は、本発明の関連技術の回路構成方法によって構成される有限体L上の演算を行う演算回路を説明するための図である。

【図2】

図2は、図1に示す有限体K上のa倍演算回路の構成図である。

【図3】

図3は、本発明の実施形態の回路構成方法によって構成される有限体L上の演算を行う演算回路を説明するための図である。

【図4】

図4は、本発明の実施形態の回路構成方法を実行するコンピュータを説明するための図である。

【図5】

図5は、図4に示すコンピュータの処理を説明するための図である。

【図6】

図6は、図3に示す有限体K上のa倍演算回路の構成図である。

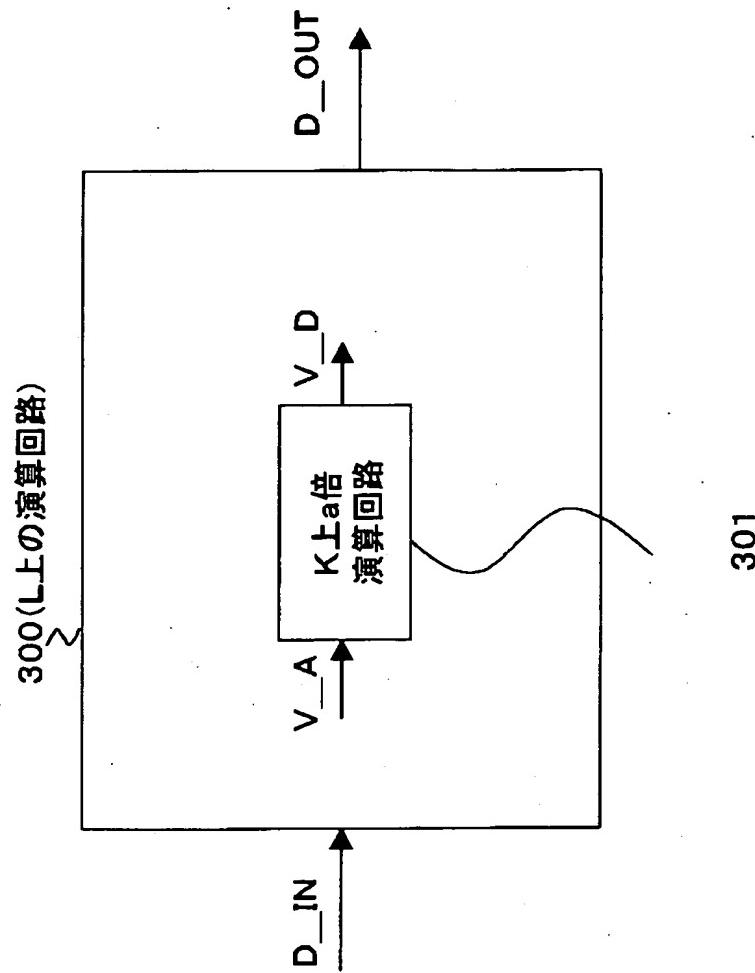
【符号の説明】

30…バス、31…操作部、32…ディスプレイ、33…メモリ、34…CPU、100, 300…有限体L上の演算回路、101, 301…有限体K上のa倍演算回路

【書類名】

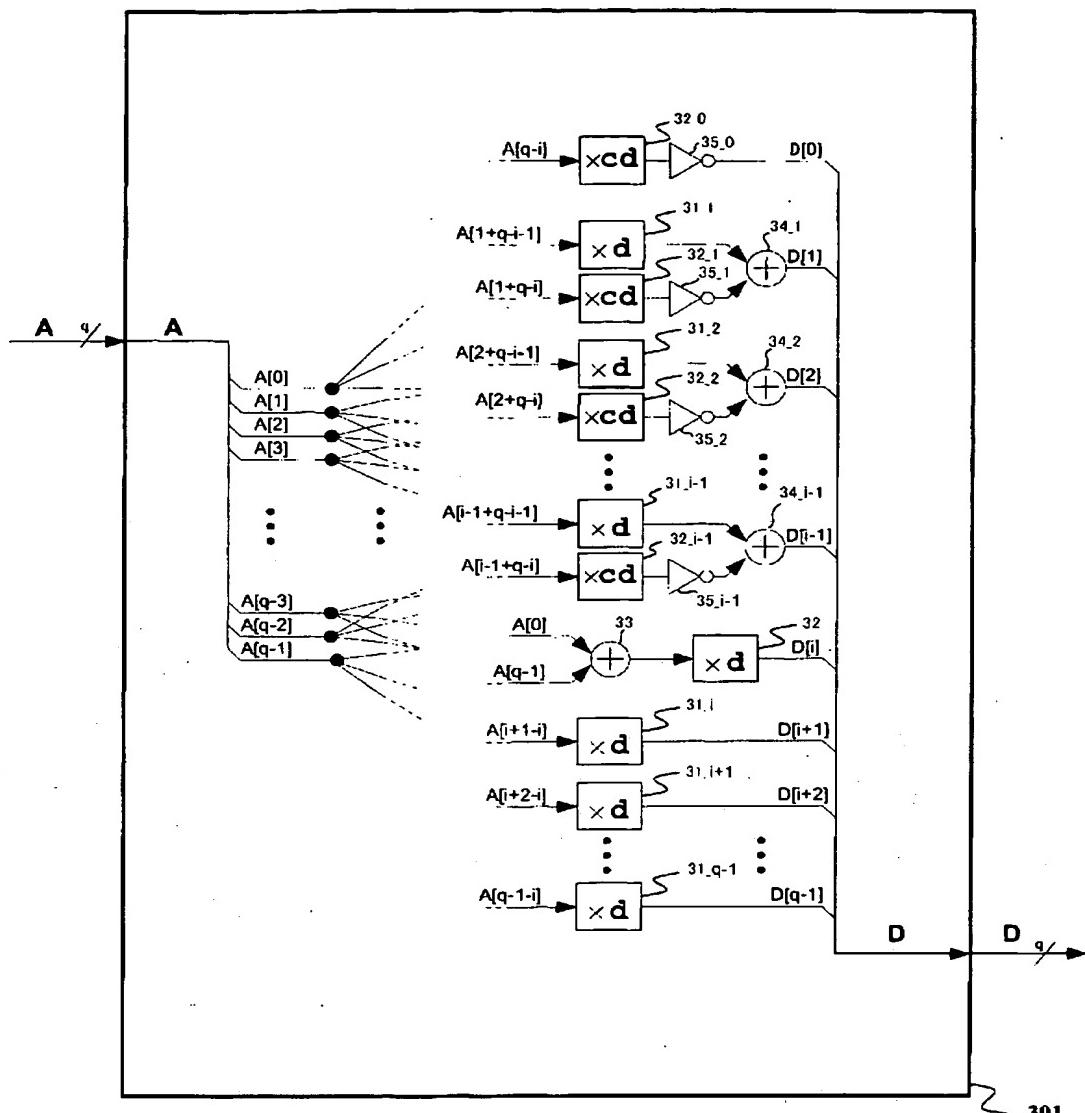
図面

【図1】



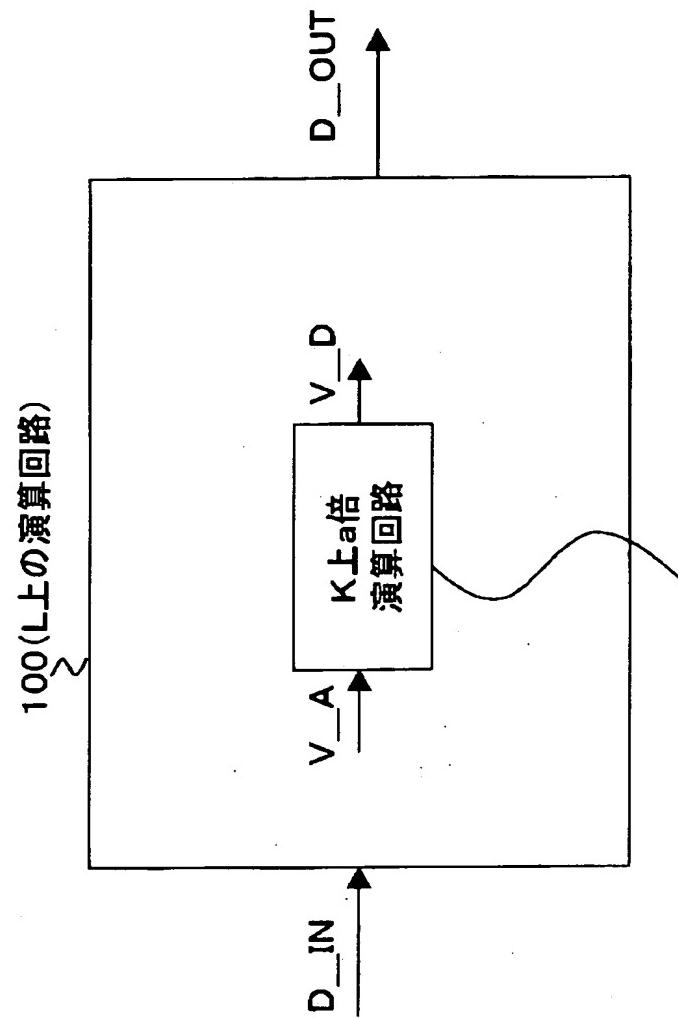
301

【図2】



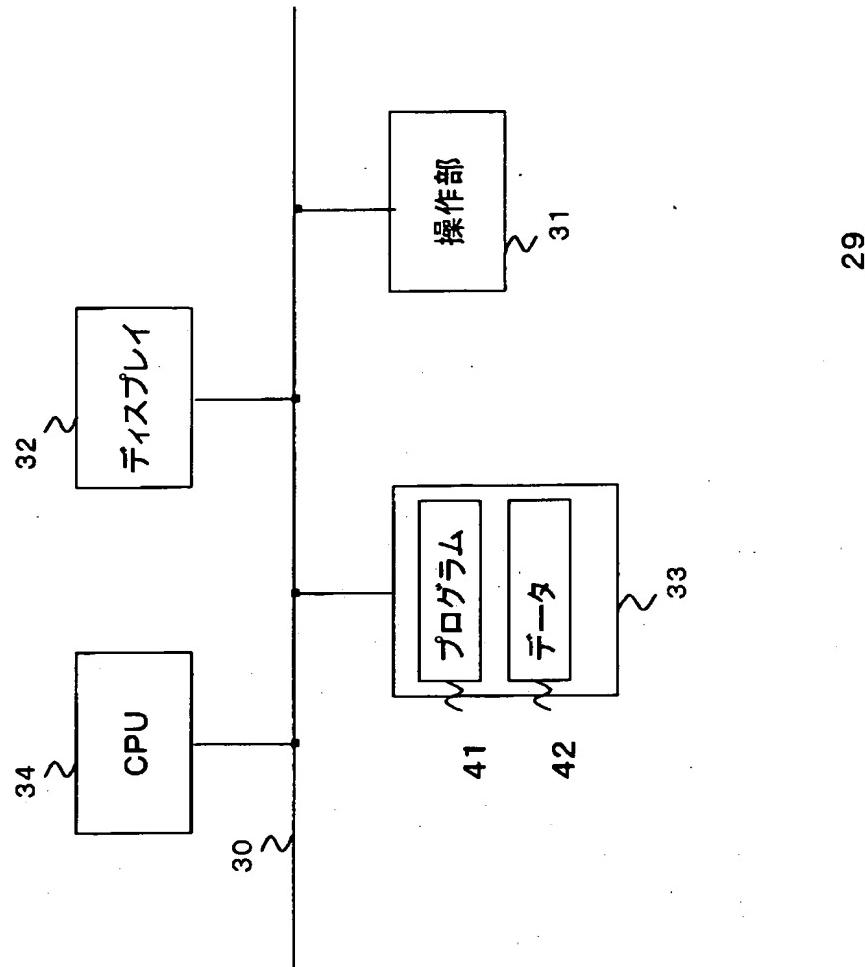
301

【図3】

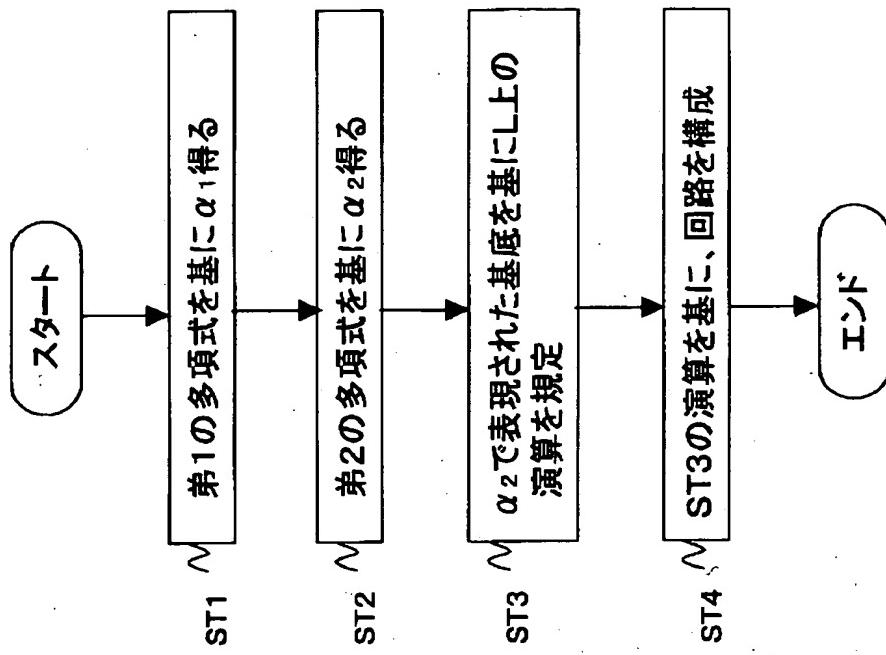


101

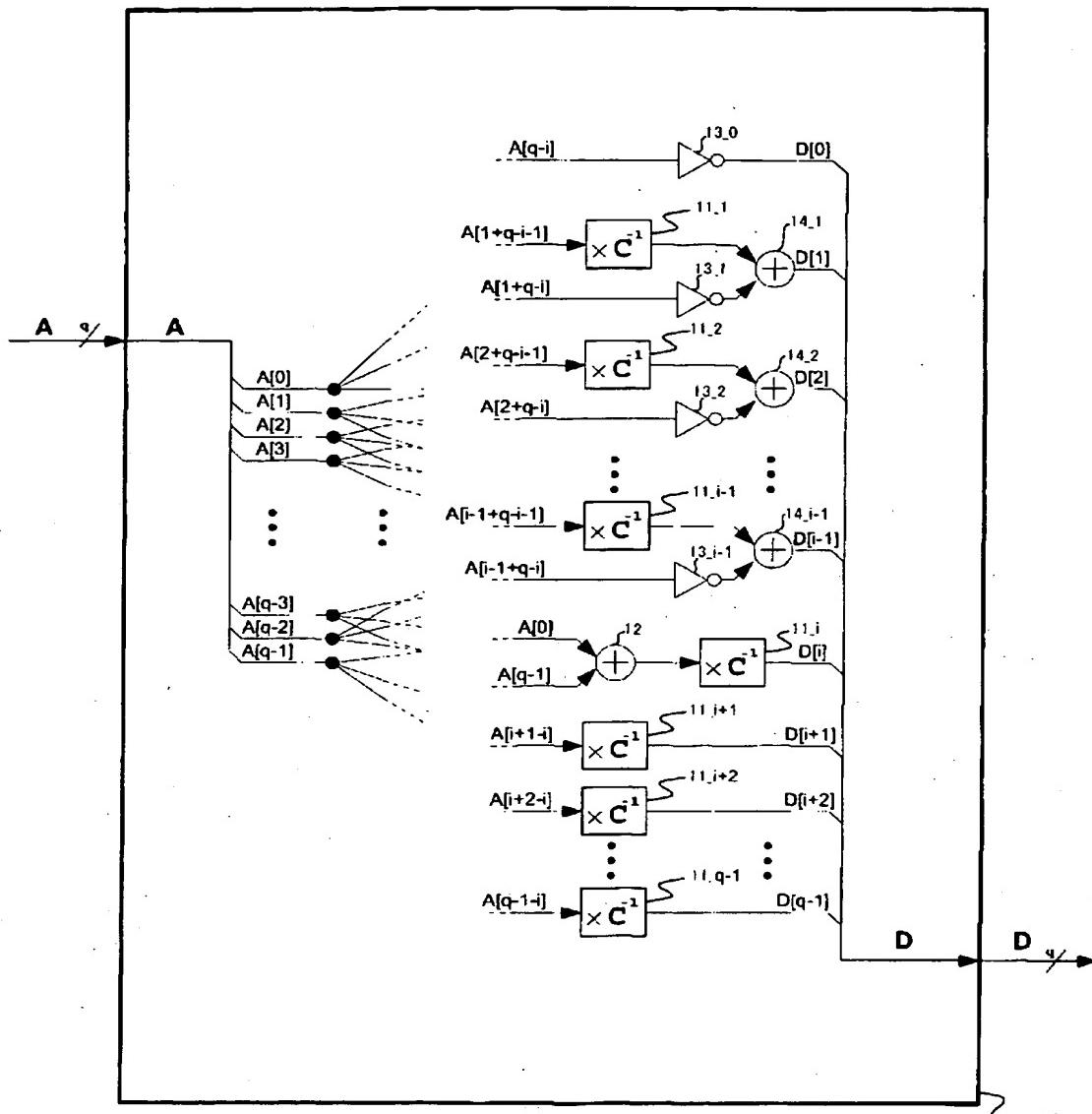
【図4】



【図5】



【図6】



101

【書類名】 要約書

【要約】

【課題】 有限体上の演算を行う演算回路を従来に比べて少ない回路構成要素で小規模に構成できる回路構成方法を提供する。

【解決手段】 第1の有限体から第2の有限体への第1の拡大についての第1の多項式を基に第1の原始根 α_1 を得る(ST1)。第2の有限体から第3の有限体への第2の拡大についての第2の多項式であって、ST1で得られた第1の原始根 α_1 と第1の多項式の0次の項の係数とを用いて、0次の項の係数が規定された第2の多項式を基に第2の原始根 α_2 を得る(ST2)。第2の原始根 α_2 を用いて表現された基底を用いて、第3の有限体上の演算を規定して演算回路を構成する(ST3, 4)。

【選択図】 図5

特願2002-330569

出願人履歴情報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社